

Degenerate asymmetric quantum concatenated codes for correcting biased quantum errors

Ji-Hao Fan(樊继豪), Jun Li(李骏), Han-Wu Chen(陈汉武), and Wen-Jie Liu(刘文杰)
Citation: Chin. Phys. B, 2021, 30 (**12**): 120302. DOI: 10.1088/1674-1056/ac05a8
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Degenerate asymmetric quantum concatenated codes for correcting biased quantum errors

Ji-Hao Fan(樊继豪), Jun Li(李骏), Han-Wu Chen(陈汉武), and Wen-Jie Liu(刘文杰)
Chin. Phys. B, 2021, 30 (**12**): 120302. DOI: 10.1088/1674-1056/ac05a8

Quantum multicast schemes of different quantum states via non-maximally entangled channels with multiparty involvement

Yan Yu(于妍), Nan Zhao(赵楠), Chang-Xing Pei(裴昌幸), and Wei Li(李玮)
Chin. Phys. B, 2021, 30 (**9**): 090302. DOI: 10.1088/1674-1056/abeef2

Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme

Jing-Wen Zhang(张静文), Xiu-Bo Chen(陈秀波), Gang Xu(徐刚), and Yi-Xian Yang(杨义先)
Chin. Phys. B, 2021, 30 (**7**): 070309. DOI: 10.1088/1674-1056/ac003b

Taking tomographic measurements for photonic qubits 88 ns before they are created

Zhibo Hou(侯志博), Qi Yin(殷琪), Chao Zhang(张超), Han-Sen Zhong(钟翰森), Guo-Yong Xiang(项国勇), Chuan-Feng Li(李传锋), Guang-Can Guo(郭光灿), Geoff J. Pryde, and Anthony Laing
Chin. Phys. B, 2021, 30 (**4**): 040304. DOI: 10.1088/1674-1056/abe29c

Nonlocal advantage of quantum coherence in a dephasing channel with memory

Ming-Liang Hu(胡明亮), Yu-Han Zhang(张宇晗), and Heng Fan(范桁)
Chin. Phys. B, 2021, 30 (**3**): 030308. DOI: 10.1088/1674-1056/abcf4a

---

Degenerate asymmetric quantum concatenated codes for correcting biased quantum errors*

Ji-Hao Fan(樊继豪)[1,†], Jun Li(李骏)[1,‡], Han-Wu Chen(陈汉武)[2], and Wen-Jie Liu(刘文杰)[3]

[1] School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
[2] School of Computer Science and Engineering, Southeast University, Nanjing 211189, China
[3] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

(Received 12 April 2021; revised manuscript received 14 May 2021; accepted manuscript online 27 May 2021)

In most practical quantum mechanical systems, quantum noise due to decoherence is highly biased towards dephasing. The quantum state suffers from phase flip noise much more seriously than from the bit flip noise. In this work, we construct new families of asymmetric quantum concatenated codes (AQCCs) to deal with such biased quantum noise. Our construction is based on a novel concatenation scheme for constructing AQCCs with large asymmetries, in which classical tensor product codes and concatenated codes are utilized to correct phase flip noise and bit flip noise, respectively. We generalize the original concatenation scheme to a more general case for better correcting degenerate errors. Moreover, we focus on constructing nonbinary AQCCs that are highly degenerate. Compared to previous literatures, AQCCs constructed in this paper show much better parameter performance than existed ones. Furthermore, we design the specific encoding circuit of the AQCCs. It is shown that our codes can be encoded more efficiently than standard quantum codes.

Keywords: asymmetric quantum codes, concatenated code, quantum channel, degenerate code

PACS: 03.67.Lx, 03.67.Pp **DOI:** 10.1088/1674-1056/ac05a8

1. Introduction

During the process of quantum computation and communication,[1,2] quantum states are inevitable to be infected by the environment noise from decoherence.[3] Quantum error correction codes (QECCs) are therefore necessary to protect quantum information from decoherence noise due to the environment interactions. Similar to classical error correction codes, how to construct QECCs with good parameters and efficient encoding/decoding algorithms is an important and difficult problem.[4] Although QECCs are highly related to classical error correction codes, the construction of QECCs is not easy at all and it seems more difficult than constructing classical error correction codes. One of the reasons is that there exists an additional dual containing (sometimes called orthogonal) restriction for constructing QECCs. In addition, there exists a striking characteristic in quantum coding theory called error degeneracy, which makes QECCs different from classical error correction codes in principle. It is assumed that degenerate codes have a large potential to correct more quantum errors than nondegenerate codes.[5,6] How to utilize such interesting feature of quantum information to improve the performance of QECCs is a large challenge in quantum coding theory.[4,6]

Recent studies show that quantum noise in many practical quantum channel models is highly biased towards dephasing errors (Z-errors) rather than amplitude errors (X-errors),[7,8] *i.e.*, there exists a large asymmetry of the happening probabilities for Z-errors and X-errors. In order to take advantage of such important prior information of quantum channels, asymmetric quantum codes (AQCs) are designed and constructed to have a biased error correction ability. For example, in Ref. [9], pure asymmetric quantum maximum-distance separable (MDS) codes with optimal parameters were constructed from two classical MDS codes whose parity-check matrix (PCM) satisfying the orthogonal restriction. In Ref. [10], asymptotically good AQCs were constructed from the dual containing algebraic-geometry (AG) codes. In Refs. [11,12], nonbinary AQCs with a large asymmetry were derived by using nested codes from the Hermitian curve. Recently, biased errors are considered in fault tolerant quantum computation (FTQC)[13,14] and topological codes,[8,15,16] in which the asymmetry can help to improve the fault tolerant threshold largely.

AQCs with a large asymmetry are extremely useful for quantum channels with highly biased noise. As the channel asymmetry is large, the Z-error correction abilities of AQCs become much more dominant. For example, very large performance gains are obtained in the FTQC threshold computation for surface codes by considering biased noise.[8,15,16] But constructing AQCs with a large asymmetry, *i.e.*, a relatively large Z-distance is quite difficult due to the orthogonal restriction. Recently, several classes of AQCs with big asymmetries

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61802175, 61871120, 61872184, and 62071240) and the Fundamental Research Funds for the Central Universities, China (Grant No. NZ2020021).

†Corresponding author. E-mail: jihao.fan@outlook.com
‡Corresponding author. E-mail: jun.li@njust.edu.cn

© 2021 Chinese Physical Society and IOP Publishing Ltd

were obtained in Ref. [20] by utilizing classical tensor product codes (TPCs)[17,18] and concatenated codes (CCs).[19] However, the authors in Ref. [20] only considered error degeneracy in X-errors, the situation in Z-errors is still unknown. In addition, only binary AQCs with good parameters are explicitly constructed in Ref. [20], the nonbinary case is not given while nonbinary QECCs are of significantly theoretical interest and are important in fault tolerant quantum computation and communication.[5,21]

In this work, we generalize the concatenation scheme in Ref. [20] to a more general case and construct new asymmetric quantum concatenated codes (AQCCs) by considering error degeneracy not only in X-errors but also in Z-errors. Therefore, we can use many existed construction results about degenerate codes, *e.g.*,[11,12,22] to facilitate our construction. As a contrast, the construction scheme in Ref. [20] only consider error degeneracy in X errors. Moreover, we give explicit constructions of nonbinary AQCs by using nonbinary constituent codes in TPCs and CCs. It is known that the performance of TPCs and CCs is highly determined by the classical constituent codes. Nonbinary codes over a larger field usually have much better parameters than binary codes. Compared with previous results, our AQCCs can have much better parameters than the existed AQCs in the previous literatures. In special, we use algebraic geometry (AG) codes as outer constituent codes to construct AQCCs and obtain several highly degenerate AQCs which have a large asymmetry. In such case, we show that the pure minimum distance of AQCCs without considering error degeneracy is constant while the true minimum distance is linear to the code length.

We present the general encoding circuit of AQCCs. We show that the amount of quantum gates needed for encoding AQCCs is bounded by $O(n_1n_2^2+n_2n_1^2)$, where n_1 and n_2 are the code length of the inner constituent code and the outer constituent code, respectively. Compared with the case for encoding general stabilizer codes which is bounded by $O(n_1^2n_2^2)$, our codes need fewer quantum gates for the encoding. Moreover, we the amount of quantum gates of encoding AQCCs can be linear to the block length provided that the corresponding classical constituent codes can be encoded linearly.

2. Theory and construction

We first present some basic knowledge and notations about AQCs, TPCs and CCs. Let q be the power of a prime number p. Denote by $GF(q)$ the Galois field which has q elements and let the field $GF(q^m)$ be the field extension of the basis field $GF(q)$, where $m>0$ is some positive integer. Denote by $\mathbb{C}$ the complex number field. For a positive integer n, denote the Hilbert space $H_n=(\mathbb{C}^q)^{\otimes n}=\mathbb{C}^{q^n}$ as the tensor product of n copies of $\mathbb{C}^q$. A q-ary quantum stabilizer code with parameters $\mathcal{Q}=[[n,k,d]]_q$ is a subspace of V_n with the dimension q^k. $\mathcal{Q}$ can detect up to $d-1$ qudits of quantum errors for $d\geq 1$.

The Calderbank–Shor–Steane (CSS) construction in Ref. [23] is a useful way to derive quantum stabilizer codes from two classical linear codes satisfying the dual containing restriction. Denote by d_x and d_z two positive integers. The asymmetric quantum code can be defined as a CSS code with parameters $Q=[[n,k,d_z/d_x]]_q$, if Q is able to detect any X-error of weight less than d_x, and any Z-error of weight less d_z. Then AQCs can be constructed from two classical error correction codes whose PCMs satisfying the orthogonal restriction based on the CSS construction.[7,23]

Lemma 1 (Ref. [7] Lemma 3.1)

For two classical q-ary linear codes with parameters $C_1=[n,k_1,d_1]_q$ and $C_2=[n,k_2,d_2]_q$ which satisfy the dual containing restriction $C_1^{\perp}\subseteq C_2$, there is an AQC whose parameters are given by $Q=[[n,k_1+k_2-n,d_z/d_x]]_q$, where

$$d_z=\max\{\mathrm{wt}(C_2\backslash C_1^{\perp}),\mathrm{wt}(C_1\backslash C_2^{\perp})\}\geq\max\{d_1,d_2\},$$
$$d_x=\min\{\mathrm{wt}(C_2\backslash C_1^{\perp}),\mathrm{wt}(C_1\backslash C_2^{\perp})\}\geq\min\{d_1,d_2\}.$$

If $d_z=\max\{d_1,d_2\}$ and $d_x=\min\{d_1,d_2\}$, then Q is a nondegenerate code, otherwise it is a degenerate code.

Next we introduce the concept of TPCs and CCs. Let $T_1=[n_1,k_1,d_1]_q$ be any classical q-ary linear code with a PCM H_{T_1}. Let $T_2=[n_2,k_2,d_2]_{q^{r_1}}$ be a q^{r_1}-ary code over the extension field $GF(q^{r_1})$ with a PCM H_{T_2}. Let $r_1=n_1-k_1$ and $r_2=n_2-k_2$ be the numbers of parity checks of T_1 and T_2, respectively. Denote by $C_T=T_2\otimes_T T_1$ the TPC of T_1 and T_2 which are the inner and outer constituent codes, respectively. Then we have $C_T=[n_1n_2,n_1n_2-r_1r_2]$. Map the elements of H_{T_1} from $GF(q)$ to $GF(q^{r_1})$. H_{T_1} can be seen as a $1\times n_1$ matrix with elements over $GF(q^{r_1})$. We can obtain an alternative representation of H_{T_1} with size $1\times n_1$. Then the PCM of C_T can be obtained as the Kronecker product of H_{T_1} and H_{T_2}, *i.e.*, $H_T=H_{T_2}\otimes H_{T_1}$. On the other hand, the PCM of TPC C_T can also be represented by a so-called companion matrix (CM) form in Refs. [24,25], $H_T=[H_{T_2}]\otimes H_{T_1}$, where $[H_{T_2}]$ is the representation of a companion matrix of H_{T_2}.

Concatenated codes are obtained by combining an inner code $D_1=[n_1,k_1,d_1]_q$ with an outer code $D_2=[n_2,k_2,d_2]_{q^{k_1}}$ over the extension field $GF(q^{k_1})$. Denote the concatenation of D_1 and D_2 by $C_C\equiv D_2\otimes_C D_1$ whose parameters are given by $C_C=[n_1n_2,k_1k_2,D\geq d_1d_2]_q$. In general, the encoding of CCs can be carried out by the outer encoding and then the inner encoding.[19] Correspondingly, the decoding of CCs is done first by the inner decoding and followed by the outer decoding. But in quantum codes, we have to do the dual containing verification and the syndrome decoding, therefore we need the exact representation generator matrix and PCM of CCs. According to Ref. [25], the generator matrix of CCs can be given in a CM form $G_C=[G_{D_2}]\otimes G_{D_1}$, where G_{D_1} and G_{D_2} are the

generator matrices of D_1 and D_2, respectively. The PCM of CCs can be given by

$$H_{C_C} = \begin{pmatrix} [H_{D_2}] \otimes (I_{k_1}, \mathbf{0}) \\ [I_{n_2}] \otimes H_{D_1} \end{pmatrix}, \tag{1}$$

where H_{D_1} and H_{D_2} are the PCMs of the inner code D_1 and the outer code D_2, respectively.

In Ref. [20], a novel concatenation scheme was proposed to facilitate the construction of AQCs, in which CCs are used for correcting the Z-errors while TPCs are used for correcting the X-errors. Denote by $C_1 = [n_1, k_1, d_1]_q$ any classical q-ary linear code with a PCM H_1 and a generator matrix G_1. For two q^{k_1}-ary codes over the extended field $GF(q^{k_1})$, denote by $C_2 = [n_2, k_2, d_2]_{q^{k_1}}$ and denote by $C_3 = [n_2, k_3, d_3]_{q^{k_1}}$. Let the PCMs of C_2 and C_3 be H_2 and H_3, respectively, and let the generator matrices of them be G_2 and G_3, respectively. Denote the tensor product code of $C_1^{\perp}$ and C_2 by $C_T = C_2 \otimes_T C_1^{\perp}$, and denote the concatenated code of C_1 and C_3 by $C_C = C_3 \otimes_C C_1$. Then there exists the following result about the construction of AQCs by unifying C_C and C_T together.

Theorem 1 (Ref. [20]) If $C_2^{\perp} \subseteq C_3$, there exists a class of AQCs whose parameters are given by $Q_A = [[n_1 n_2, K, d_z \geq d_1 d_3/d_x \geq d_2]]_q$, where $K = k_1(k_2 + k_3 - n_2)$.

In Ref. [20], Theorem 1 can be used to derive AQCs with large Z-distances and efficient decoding algorithms. However, Theorem 1 only considered the error degeneracy phenomenon in the inner codes while the case the case in the outer code was not considered. In this work, we generalize the result in Ref. [20] to a more general situation by considering error degeneracy in both the inner and the outer codes, and we have the following generalized result.

Theorem 2 There exists a class of AQCCs whose parameters are given by $Q_A = [[n_1 n_2, K, d_z/d_x]]_q$, where $K = k_1(k_2 + k_3 - n_2)$, $d_z \geq d_1 \mathrm{wt}(C_3 \backslash C_2^{\perp})$, and $d_x \geq \mathrm{wt}(C_2 \backslash C_3^{\perp})$.

Proof We first compute the X-distance d_x. Denote the X-error that happening in the codeword by e_X. Similar to the proof of Theorem 1 in Ref. [20], the syndrome information Υ of X-errors is given by $\Upsilon = [H_2^t] \otimes G_1 \cdot e_X^{\mathrm{T}}$. Denote by $\Upsilon_{\mathrm{I}_i} \equiv G_1 e_{X_i}^{\mathrm{T}}, 1 \leq i \leq n_2$. Then $\Upsilon_I = (\Upsilon_{\mathrm{I}_1}, \ldots, \Upsilon_{\mathrm{I}_{n_2}})$ can be seen as the error sequence happening in the outer constituent code C_2. Then we have $\Upsilon = [H_2^t](\Upsilon_{\mathrm{I}_1}, \ldots, \Upsilon_{\mathrm{I}_{n_2}})^{\mathrm{T}}$, which is the syndrome information for the outer decoding. Suppose that we use some syndrome based decoding algorithm for the outer code C_2 to do the decoding and suppose that $\mathrm{wt}(e_X) < \mathrm{wt}(C_2 \backslash C_3^{\perp})$. Whatever the errors are separated into different subblocks in the codeword, we must have $\mathrm{wt}(\Upsilon_I) < \mathrm{wt}(C_2 \backslash C_3^{\perp})$. If there is $[H_2^t]\Upsilon_I^{\mathrm{T}} = 0$, we have $\Upsilon_I \in C_3^{\perp}$ which means that Υ_I is degenerate. Therefore if $\mathrm{wt}(e_X) < \mathrm{wt}(C_2 \backslash C_3^{\perp})$, then e_X is either undetectable but degenerate, or detectable. Thus we have $d_x \geq \mathrm{wt}(C_2 \backslash C_3^{\perp})$.

Next we consider the case of correcting Z-errors and compute the Z-distance d_z. Let e_Z be the Z-error happening in the received codeword and suppose that $\mathrm{wt}(e_Z) < d_1 \mathrm{wt}(C_3 \backslash C_2^{\perp})$. If the number of erroneous subblocks of the outer code is less than $\mathrm{wt}(C_3 \backslash C_2^{\perp})$, then we can always detect the errors or the errors are undetectable but degenerate. If the number of erroneous subblocks is larger than or equal to $\mathrm{wt}(C_3 \backslash C_2^{\perp})$, we know that there exists at least one erroneous subblock which has at most $d_1 - 1$ errors since we have assumed that $\mathrm{wt}(e_Z) < d_1 \mathrm{wt}(C_3 \backslash C_2^{\perp})$. In such a situation, we might cannot detect the erroneous subblocks of the outer code. Because the number of erroneous subblocks is larger than or equal to $\mathrm{wt}(C_3 \backslash C_2^{\perp})$, which exceeds the error detection ability of the outer code. However we can always detect the error by using the inner code since there is still at least one erroneous subblock whose error weight is less than $d_1 - 1$ and it is detectable. Therefore we know that the Z-distance $d_z \geq d_1 \mathrm{wt}(C_3 \backslash C_2^{\perp})$. □

Compared to Theorem 1 in Ref. [20], Theorem 2 can have better parameters since we can use degenerate outer codes to do the construction. In Refs. [11,12], several classes of AQCs with big minimum distance are constructed from nested code pairs but those AQCs are unknown whether degenerate or not. Thus the results in Refs. [11,12] were unknown whether can be used to construct AQCs by using Theorem 1 in Ref. [20]. We solve this problem by using Theorem 2 and we can use the codes in Refs. [11,12] as the outer codes to construct AQCCs in this work. First, we review some construction results in Refs. [11,12].

Theorem 3 Let $l \geq 2$ be integers and let $s \leq q$, in which q is a prime power. Given $\delta \in \{1, \ldots, s^l\}$, and let $v \in \{0, \ldots, l-1\}$ be such that $s^v \leq \delta \leq s^{v+1}$ and choose an integer $\delta^{\perp} \leq \lfloor (s - \delta/s^v + 1) s^{l-v-1} \rfloor$. Denote by

$$f \geq s^l - \sum_{i=1}^{l} \frac{1}{(i-1)!} (\delta(\ln(s^l/\delta))^{i-1} + \delta^{\perp}(\ln(s^l/\delta^{\perp}))^{i-1}). \tag{2}$$

There exists a class of AQCs with parameters

$$[[n = s^l, f, d_z \geq \delta/d_x \geq \delta^{\perp}]]_q. \tag{3}$$

Proof See the proof of Theorem 24 in Ref. [11].

With the notations given above, we can obtain the the construction of AQCCs as follows.

Corollary 1 There is a class of AQCCs with parameters $Q = [[n_1 n_2, K, d_z/d_x]]_q$, where $K = k_1(k_2 + k_3 - n_2)$, $d_z \geq d_1 \delta$, and $d_x \geq \delta^{\perp}$.

In Ref. [11], several classes of nonbinary AQCs with better parameters than the codes in Refs. [26,27] were constructed based on Theorem 3. We take $C_1 = [n_1, 1, n_1]_q$ as the inner codes and let the outer codes be AQCs listed in Ref. [11] and we construct new nonbinary AQCCs by using Corollary 1. In Table 1, we list the new results and also make comparisons with AQCs in Ref. [26]. It is shown that our new AQCCs have better parameters than the AQCs in Ref. [26].

Table 1. Comparisons of AQCCs with previous works in Ref. [26]. The AQCCs are derived from Corollary 1.

m_1	AQCCs	Ref. [26]	m_1	AQCCs	Ref. [26]
6	$[[147,3,90/4]]_7$	$[[147,3,46/4]]_7$	7	$[[128,5,70/5]]_8$	$[[128,4,28/5]]_8$
6	$[[147,8,72/4]]_7$	$[[147,6,45/4]]_7$	7	$[[128,12,60/4]]_8$	$[[128,8,28/4]]_8$
6	$[[147,5,72/5]]_7$	$[[147,3,45/5]]_7$	7	$[[128,9,60/5]]_8$	$[[128,8,27/5]]_8$
6	$[[147,9,60/5]]_7$	$[[147,9,43/5]]_7$	7	$[[128,7,60/6]]_8$	$[[128,4,27/6]]_8$
6	$[[147,10,42/7]]_7$	$[[147,9,41/7]]_7$	7	$[[128,10,50/6]]_8$	$[[128,8,26/6]]_8$
6	$[[147,14,42/6]]_7$	$[[147,12,41/6]]_7$	7	$[[128,10,48/7]]_8$	$[[128,8,25/7]]_8$
6	$[[147,3,72/8]]_7$	$[[147,3,42/8]]_7$	7	$[[192,5,105/5]]_8$	$[[192,3,60/5]]_8$
6	$[[147,4,52/10]]_7$	$[[147,3,40/10]]_7$	7	$[[192,12,90/4]]_8$	$[[192,12,58/4]]_8$
6	$[[147,3,45/15]]_7$	$[[147,3,35/15]]_7$	7	$[[192,9,90/5]]_8$	$[[192,9,58/5]]_8$
6	$[[147,5,36/12]]_7$	$[[147,3,35/12]]_7$	7	$[[192,7,90/6]]_8$	$[[192,6,61/5]]_8$
6	$[[84,4,40/5]]_7$	$[[84,2,38/5]]_7$	7	$[[192,10,75/6]]_8$	$[[192,9,57/6]]_8$
6	$[[84,9,36/4]]_7$	$[[84,8,36/4]]_7$	7	$[[192,10,72/7]]_8$	$[[192,9,56/7]]_8$

It should be noticed that one of the key points to construct highly degenerate AQCCs is by choosing the constituent codes C_1 with a relatively large minimum distance. Therefore we use some best known nonbinary linear codes in Ref. [28] to construct AQCCs with a large asymmetry, *i.e.*, a large minimum distance d_z. For example, we can choose $C_1=[5,3,3]_4$. Let $C_2=[n_2,k_2,d_2]_{4^3}$ and let $C_3=[n_2,k_3,d_3]_{4^3}$ be MDS codes over $GF(4^3)$, where $k_2+k_3>n_2$ and $3\leq n_2\leq 4^3+1$. Then according to Ref. [4], there is $C_2^{\perp}\subseteq C_3$ and then there exist AQCCs with parameters $[[5n_2,3(k_2+k_3-n_2),3d_3/d_2]]_4$ according to Theorem 2. Then we can obtain, *e.g.*, AQCCs with parameters $[[35,6,15/2]]_4$, $[[35,3,9/5]]_4$ which are better than $[[35,5,15/2]]_4$, $[[35,3,8/5]]_4$ in Ref. [29], respectively. In Table 2, we list more nonbinary AQCCs based on the online codes in Ref. [28]. It is shown that our AQCCs have better parameters than AQCs in Ref. [29].

Table 2. Comparisons of AQCCs with best known AQCs in Ref. [29].

C_1	C_2	C_3	AQCCs	Ref. [29]
$[4,2,3]_4$	$[6,5,2]_{16}$	$[6,2,5]_{16}$	$[24,2,15/2]_4$	$[25,2,15/2]_4$
$[4,2,3]_4$	$[11,9,3]_{16}$	$[11,4,8]_{16}$	$[44,4,24/3]_4$	$[45,3,10/3]_4$
$[4,2,3]_4$	$[11,10,2]_{16}$	$[11,4,8]_{16}$	$[44,6,24/2]_4$	$[45,5,21/2]_4$
$[4,2,3]_4$	$[12,11,2]_{16}$	$[12,3,10]_{16}$	$[48,4,30/2]_4$	$[49,3,21/2]_4$
$[5,3,3]_4$	$[7,6,2]_{4^3}$	$[7,3,5]_{4^3}$	$[35,6,15/2]_4$	$[35,5,15/2]_4$
$[5,3,3]_4$	$[7,3,5]_{4^3}$	$[7,5,3]_{4^3}$	$[35,3,9/5]_4$	$[35,3,8/5]_4$
$[6,3,4]_4$	$[5,4,2]_{4^3}$	$[5,2,4]_{4^3}$	$[30,3,16/2]_4$	$[31,4,15/2]_4$
$[6,3,4]_4$	$[8,7,2]_{4^3}$	$[8,2,7]_{4^3}$	$[48,3,28/2]_4$	$[49,3,21/2]_4$

Next, we use the dual of repetition codes which are usually called even weight codes as the inner codes to construct TPCs and CCs. The even weight codes are MDS codes and are thus optimal. We have the following construction of nonbinary AQCCs.

Proposition 1 Let $C_1=[m,m-1,2]_q$ be the even weight code with $m\geq 2$ and $q\geq 3$ which are integers. There exists a class of nonbinary AQCCs with parameters

$$Q_E=[[mn,(m-1)(n-d_2-d_3+2),d_z\geq 2d_3/d_x\geq d_2]]_q, \quad (4)$$

where $2\leq n\leq q^{m-1}+1$ and $2\leq d_1+d_2\leq n+2$ are all integers.

Proof Let $C_2=[n,n-d_2+1,d_2]_{q^{m-1}}$ and $C_3=[n,n-d_3+1,d_3]_{q^{m-1}}$ be two classical MDS codes over the extended field $GF(q^{m-1})$. If $2\leq n\leq q^{m-1}+1$ and $2\leq d_2+d_3\leq n+2$, then there are C_2 and C_3 satisfying the dual containing relationship such that $C_2^{\perp}\subseteq C_3$. According to Theorem 2, there exists a class of AQCCs with parameters $[[mn_2,(m-1)(n-d_1-d_2+2),2d_2/d_1]]_q$. □

In Ref. [20], binary AQCs constructed from TPCs and CCs were compared with the binary extension of quantum Reed–Solomon (RS) codes. Here we compare nonbinary AQCs in Proposition 1 with nonbinary AQCs obtained from the extension of quantum generalized RS (GRS) codes. In Ref. [26], the following AQCs are obtained from quantum GRS codes with parameters

$$Q_{\rm G}=[[N=mn,K=m(n-d_z-d_x+2),d_z/d_x]]_q, \quad (5)$$

where $d_x+d_z-2<n<q^m$. We take $d_z=2d_3$ and $d_x=d_2$ in Proposition 1, then $Q_{\rm E}$ and $Q_{\rm G}$ have the same length and minimum distance bound. We compare the dimensions of $Q_{\rm E}$ and $Q_{\rm G}$. Through some simple computations, we know that if

$$d_z+\frac{2}{m+1}d_x>\frac{2n+4}{m+1}, \quad (6)$$

then our codes have larger dimensions than AQCs in Ref. [26]. In Table 3, we list some AQCCs and give detailed comparison between the parameters of $Q_{\rm E}$ and $Q_{\rm G}$. AQCCs show much better parameter performance than the AQCs in Ref. [26].

It is known that classical repetition codes are optimal codes and have the largest minimum distance. If we use classical repetition codes as the inner codes, we can obtain highly degenerate AQCs with large Z-distances. On the other hand, it is an interesting but difficult problem to determine whether an AQC is degenerate or not.[4] If we use repetition codes as the inner codes, we can easily verify if the resultant AQCC is degenerate. We have the following result about the construction of highly degenerate AQCCs.

Table 3. Comparisons of AQCCs with the asymmetric QRS codes.[26] AQCCs are constructed according to Proposition 1.

q	m	n	AQCCs	Ref. [26]
5	4	27	$[[81,6,48/3]]_3$	$[[81,4,25/3]]_3$
3	4	27	$[[81,6,44/5]]_3$	$[[81,4,23/5]]_3$
3	4	27	$[[81,6,40/7]]_3$	$[[81,4,21/7]]_3$
3	4	27	$[[81,42,24/3]]_3$	$[[81,8,24/3]]_3$
3	4	27	$[[81,39,22/5]]_3$	$[[81,8,22/5]]_3$
3	4	27	$[[81,36,20/7]]_3$	$[[81,8,20/7]]_3$
3	4	27	$[[81,60,12/3]]_3$	$[[81,56,12/3]]_3$
3	4	27	$[[81,57,10/5]]_3$	$[[81,56,10/5]]_3$
5	5	626	$[[3130,8,1246/3]]_5$	$[[3130,5,624/3]]_5$
5	5	626	$[[3130,12,1240/5]]_5$	$[[3130,10,621/5]]_5$
5	5	626	$[[3130,16,1234/7]]_5$	$[[3130,15,618/7]]_5$
5	5	626	$[[3130,1264,616/4]]_5$	$[[3130,40,616/4]]_5$
5	5	626	$[[3130,1260,614/6]]_5$	$[[3130,40,614/6]]_5$
5	5	626	$[[3130,1256,612/8]]_5$	$[[3130,40,612/8]]_5$
5	5	626	$[[3130,2036,220/9]]_5$	$[[3130,1995,220/9]]_5$
5	5	626	$[[3130,2044,214/10]]_5$	$[[3130,2020,214/10]]_5$
5	5	626	$[[3130,2056,206/11]]_5$	$[[3130,2055,206/11]]_5$

Proposition 2 Let $m \geq 3$ and $q \geq 3$ be integers. Denote by $C_1 = [m,1,m]_q$ the repetition code which has the largest minimum distance. There exists a class of nonbinary AQCCs with parameters

$$Q_R = [[mn, n-d_2-d_3+2, d_z \geq md_3/d_x \geq d_2]]_q, \tag{7}$$

where $2 \leq n \leq q+1$, and $2 \leq d_2+d_3 \leq n+2$ are all integers. Further, if $d_2 \geq 3$, then Q_R is degenerate.

Proof Denote by $C_2 = [n, n-d_2+1, d_2]_q$ and $C_3 = [n, n-d_3+1, d_3]_q$ two classical MDS codes over the finite field $GF(q)$. If $2 \leq n \leq q+1$ and $2 \leq d_2+d_3 \leq n+2$, then there exist C_2 and C_3 such that $C_2^{\perp} \subseteq C_3$. Therefore there exists a class of AQCCs with parameters $[[mn_2, n-d_2-d_3+2, md_3/d_2]]_q$.

If we do not consider error degeneracy, then the pure minimum distance of Q_{R} is determined by the minimum of the dual distance of C_1 and d_2, *i.e.*, $d_x \geq \min\{d_1^{\perp}, d_2\}$. Notice that the dual distance of the repetition code is $d_1^{\perp} = 2$, then if $d_2 \geq 3$, the pure minimum distance of Q_{R} without considering error degeneracy is always 2. However the true minimum distance of Q_{R} is larger than or equal to d_2 which is larger than 2. Therefore Q_{R} is degenerate.

By using Proposition 2, we can construct nonbinary and highly degenerate AQCCs with a large Z-distance. We list parts of them as follows:

$$[[40,1,35/2]]_7,\ [[40,1,30/3]]_7,\ [[48,1,42/2]]_7,$$
$$[[48,1,36/3]]_7,\ [[63,1,56/2]]_8,\ [[63,1,49/3]]_8,$$
$$[[72,1,48/4]]_8,\ [[72,1,40/5]]_8.$$

These AQCCs all have a dimension of 1 but the Z-distance is very large.

In classical error correction codes, the algebraic geometry (AG) codes can break the classical Gilbert–Varshamov (GV) bound of nonbinary codes when field size is larger than 49.[30] We use nonbinary AG codes with large field size as the outer codes to construct asymptotically good AQCCs. Let $q = p^{2m}$ be a prime power, where $m \geq 1$ is an integer. There exists the following construction of asymmetric quantum AG codes in Ref. [10].

Theorem 4 (Ref. [10]) Let $0 \leq \delta_x, \delta_z \leq 1$ and $\delta_x + \delta_z \leq 1 - 2/(p^m - 1)$. There exists a class of q-ary asymmetric quantum AG codes Q_A such that

$$R_{Q_A} \geq 1 - \delta_x - \delta_z - \frac{2}{p^m - 1}, \tag{8}$$

where $R_{Q_{\mathrm{A}}}$ is the rate of quantum AG codes Q_{A}.

We can construct the following nonbinary AQCCs from AG codes that satisfy the restriction of dual containing.

Proposition 3 There is a class of asymptotically good q-ary AQCCs with the following asymptotic rate:

$$R_{Q_{\mathrm{A}}} \geq \frac{k_1}{n_1}\left(1 - \frac{n_1}{d_1}\delta_z - n_1\delta_x - \frac{2}{p^{mk_1} - 1}\right). \tag{9}$$

Proof Take $C_1 = [n_1, k_1, d_1]_q$ as any classical linear code over $GF(q)$. Denote $\mathcal{X}$ by an algebraic curve with genus ℓ defined over $GF(q^{k_1})$, and suppose that $\mathcal{X}$ has more than $n_2 - 1$ rational points. Denote by $2\ell - 2 < s < t < n_2$. According to (Ref. [10], Proposition 4.2), there are two AG codes over the extension filed $GF(q^{k_1})$ with parameters $C_2 = [n_2, k_2, d_2]_{q^{k_1}}$ and $C_3 = [n_2, k_3, d_3]_{q^{k_1}}$, where $k_2 = n_2 - k_3 + t - s$ such that $C_2^{\perp} \subseteq C_3$. By using Theorem 2, we can obtain a class of AQCCs with parameters $Q_{\mathrm{A}} = [[n_1 n_2, k_1(t-s), d_1 d_3/d_2]]$, where $d_2 \geq s - 2\ell + 2$, and $d_3 \geq n_2 - t$. Let δ_x and δ_z be the relatively X-distance and Z-distance of Q_{A}, respectively. Taking $n_2 \to \infty$, then we can obtain the following asymptotic result:

$$R_{Q_{\mathrm{A}}} \geq \frac{k_1}{n_1}\left(1 - \frac{n_1}{d_1}\delta_z - n_1\delta_x - \frac{2}{\sqrt{q^{k_1}} - 1}\right). \tag{10}$$

□

Denote by $\alpha = d_z/d_x = \delta_z/\delta_x$ the asymmetry of AQCCs. Taking $C_1 = [n_1, n_1 - d_1 + 1, d_1]_q$ where $2 \leq n_1 \leq q+1$ is a constant, then we have

$$R_{Q_{\mathrm{A}}} \geq \frac{n_1 - d_1 + 1}{n_1} \times \left(1 - \left(\frac{n_1}{d_1} + \frac{n_1}{\alpha}\right)\delta_z - \frac{2}{p^{m(n_1 - d_1 + 1)} - 1}\right). \tag{11}$$

We plot the curves of Eq. (11) in Fig. 1 with different field sizes. It is not difficult to see that Q_{A} is highly degenerate, since n_1 is a constant and the dual distance of C_1 is also a constant. Moreover, in the binary case, binary AQCs based on TPCs and CCs can only outperform the binary extension of asymmetric quantum AG codes.[20] Here we compare our codes with asymmetric quantum AG codes directly without needing to do the field extension. It is shown that our codes can have better performance than the asymmetric quantum AG codes in Ref. [10] in some scopes, see Fig. 1.

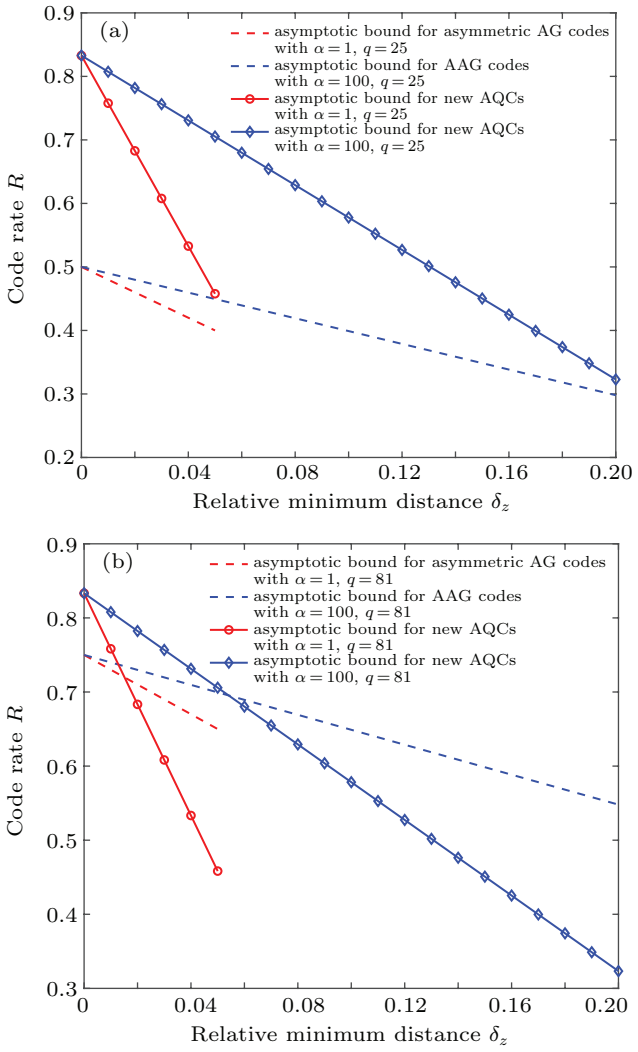


Fig. 1. The asymptotic bounds for our AQCCs in Proposition 3 and the comparison with asymmetric quantum AG codes in Ref. [10] with the field size $q=25$ and $q=81$, respectively.

3. Encoding circuits of asymmetric quantum concatenated codes

It was shown that AQCs in Theorem 1 can be efficiently decodable if the corresponding classical constituent codes can be decoded efficiently.[20] But the encoding of AQCs was not discussed in Ref. [20]. The encoding efficiency of quantum codes is not only important to fault-tolerant quantum computation but also shown to be crucial in fault-tolerant quantum communication.[21] In this section we give the encoding circuit of asymmetric quantum concatenated codes and we use the standard encoding method given in Ref. [31]. Denote the quantum basis state after the encoding by

$$|x+C_T^{\perp}\rangle \equiv \frac{1}{\sqrt{|C_T^{\perp}|}}\sum_{y\in C_T^{\perp}}|x+y\rangle, \tag{12}$$

where $x\in C_C$. Since we have assumed that $C_2^{\perp}\subseteq C_3$, then the generator matrix of C_3 can be given by

$$G_3=\begin{pmatrix} H_2 \\ \widehat{G}_3 \end{pmatrix},\ \widehat{G}_3=(\boldsymbol{O},\boldsymbol{I},P_3), \tag{13}$$

where $\boldsymbol{O}$ is a zero subblock of size $(k_3-r_2)\times r_2$, $\boldsymbol{I}$ is an identity matrix of size $(k_3-r_2)\times(k_3-r_2)$, and P_3 is a subblock of size $(k_3-r_2)\times r_3$. Then the generator matrix of C_C is given by

$$G_{C_C}=\begin{pmatrix} [H_2^t]\otimes G_1 \\ \widehat{G}_{C_C} \end{pmatrix},\quad \widehat{G}_{C_C}=[\widehat{G}_3^t]\otimes G_1. \tag{14}$$

According to the standard encoding methods given in Ref. [31], the first step of the encoding circuit of CSS codes can be carried out by using the subblock $\widehat{G}_{C_C}$ in Eq. (14). We have $x=x_0\widehat{G}_{C_C}\in C_C$. The second step for generating the superposition state of Eq. (12) is based on the generator matrix of $C_T^{\perp}$, *i.e.*, $H_{C_T}=[H_2^t]\otimes G_1$, which is just the PCM of C_T. Therefore the encoding in the second stage is the same with that of the concatenated code of $C_2^{\perp}$ and C_1. We know that $y=y_0H_{C_C}\in C_T^{\perp}$. Therefore we have

$$\begin{aligned} |x+C_T^{\perp}\rangle &= \frac{1}{\sqrt{|C_T^{\perp}|}}\sum_{y\in C_T^{\perp}}|x+y\rangle \\ &= \frac{1}{\sqrt{|C_T^{\perp}|}}\sum_{y_0}|x_0\widehat{G}_{C_C}+y_0H_{C_C}\rangle \\ &= \frac{1}{\sqrt{|C_T^{\perp}|}}\sum_{y_0}|(x_0[\widehat{G}_3^t]+y_0[H_2^t])\otimes G_1\rangle, \end{aligned} \tag{15}$$

where x_0 is the information bits corresponding to $x\in C_C$. Assume that H_2 and G_1 are represented by the standard form, *i.e.*, $H_2=[I,P_2]$ and $G_1=[I,P_1]$. Then we have the general encoding circuit of AQCCs in Fig. 2.

Now we analysis the encoding efficiency of the circuit in Fig. 2. We evaluate the total number of quantum gates in the circuit. In stage I, the number of quantum gates is determined by the density of P_3 which is $O(n_1n_2^2)$ in the worst case. Similarly in stage II, the number of quantum gates is also $O(n_1n_2^2)$ in the worst case. While in stage III, the number of quantum gates is determined by the density of P_1 and the length of the circuit, and the complexity is $O(n_2n_1^2)$. Therefore the total encoding complexity of AQCCs of block length n_1n_2 is $O(n_1n_2^2+n_2n_1^2)$ in the worst case. Compared with the complexity of encoding general stabilizer codes which is given by $O(n_1^2n_2^2)$, our codes have a lower encoding complexity. Moreover, it is easy to see that if the classical constituent codes C_1, C_2, and C_3 can be encoded efficiently in linear time, for example, P_1, P_2, and P_3 are with low density, then the encoding complexity of AQCCs is $O(n_1n_2)$. Thus AQCCs can also be encoded efficiently in linear time provided that the constituent codes are efficiently encodable.

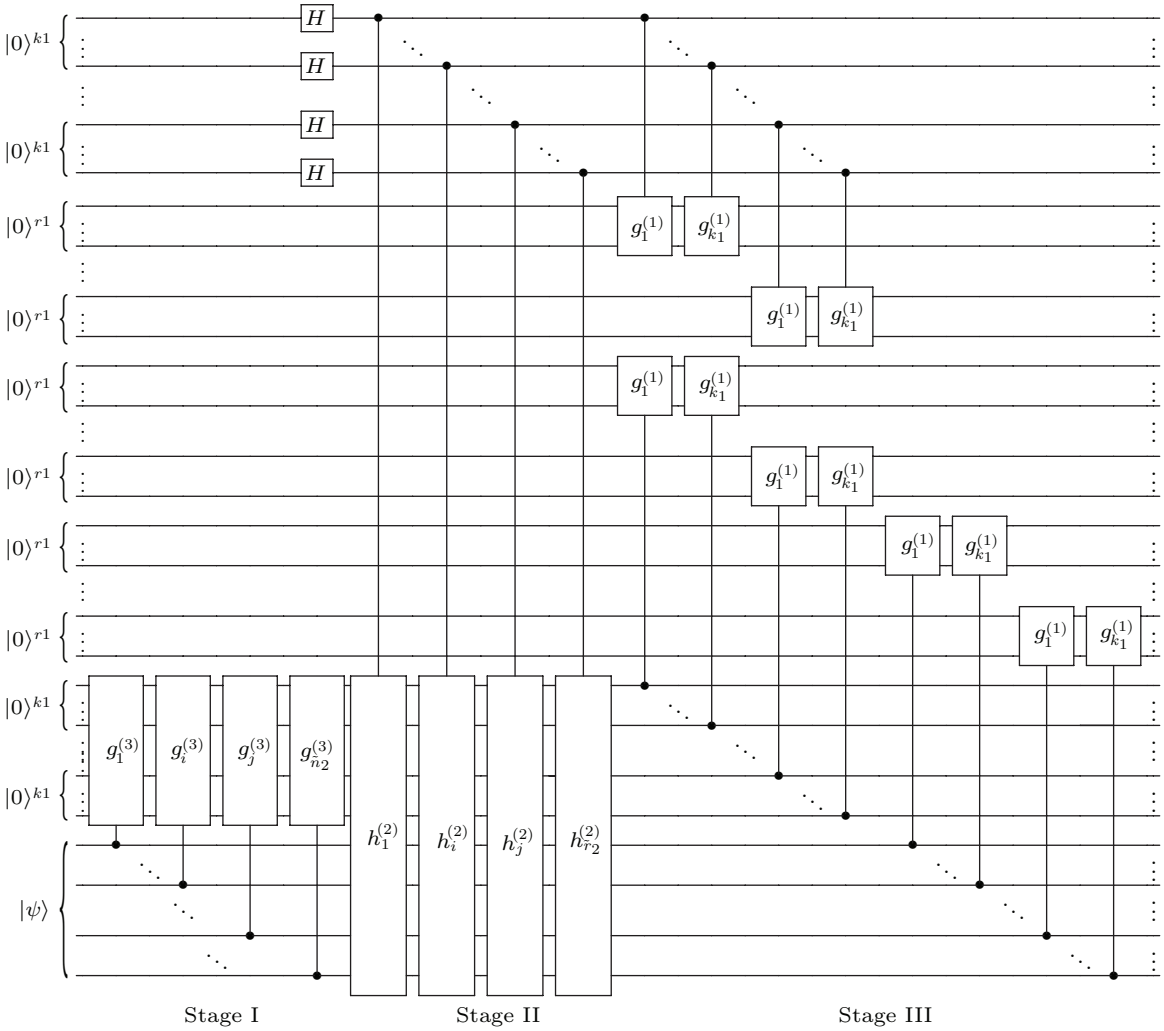


Fig. 2. The encoding circuit of asymmetric quantum concatenated codes. In stage I, the block labeled by $g_i^{(3)}(1 \le i \le \widetilde{n}_2)$ means that the qubits pass it are controlled by a qubit in quantum state $|\psi\rangle$. If there is a "1" in the j-th position of the i-th row of P_3, then there is a C-NOT target "$\otimes$" in the j-th quantum state of the subblock $g_i^{(3)}$, *i.e.*, each $g_i^{(3)}$ corresponds to a row of $[P_3^t]$. Similarly, each $h_i^{(2)}(1 \le i \le \widetilde{r}_2)$ in stage II corresponds to a row of $[P_2^t]$, and each $g_i^{(1)}(1 \le i \le \widetilde{k}_1)$ in stage III corresponds to a column of $[P_1]$.

We give an explicit example to illustrate the encoding of AQCCs. Let $C_1 = [3,2,2]$ be the even weight code. Let C_2, C_3 be two 4-ary codes with parameters $[5,3,3]_4$ and they satisfy $C_2^{\perp} \subseteq C_3$.[32] The generator matrix and the PCM of C_1 are given by

$$G_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad H_1 = (1\ 1). \tag{16}$$

The generator matrices and PCMs of C_2 and C_3 are given as follows:

$$\begin{aligned} G_2 &= \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha \\ 0 & 1 & 0 & \alpha & \alpha \\ 0 & 0 & 1 & \alpha & 1 \end{pmatrix}, \\ H_2 &= \begin{pmatrix} 1 & 0 & 1 & \alpha & \alpha \\ 0 & 1 & \alpha & \alpha & 1 \end{pmatrix}, \\ G_3 &= \begin{pmatrix} 1 & 0 & 0 & 1 & \alpha^2 \\ 0 & 1 & 0 & \alpha^2 & \alpha^2 \\ 0 & 0 & 1 & \alpha^2 & 1 \end{pmatrix}, \end{aligned} \tag{17}$$

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \end{pmatrix}, \tag{18}$$

where α is the primitive element of $GF(4)$. It is easy to verify that $H_2 H_3^{\mathrm{T}} = 0$. Then we can obtain an AQCC with parameters $Q = [[15,2,6/3]]$. The generator matrix G_3 is equivalent to the following one under some elementary row transformations:

$$G_3 \to \begin{pmatrix} H_2 \\ \widehat{G}_3 \end{pmatrix}, \quad \widehat{G}_3 = [0\,0\,\mathbf{1}\,\alpha^2\,1]. \tag{19}$$

The elements $0, 1, \alpha, \alpha^2$ of $GF(4)$ can be represented by the companion matrix form of the primitive polynomial $f(x) = 1 + x + x^2$ as follows (see Refs. [24,25]):

$$\begin{aligned} O &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad M^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ M &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned} \tag{20}$$

Then the encoding circuit of this code is given in Fig. 3.

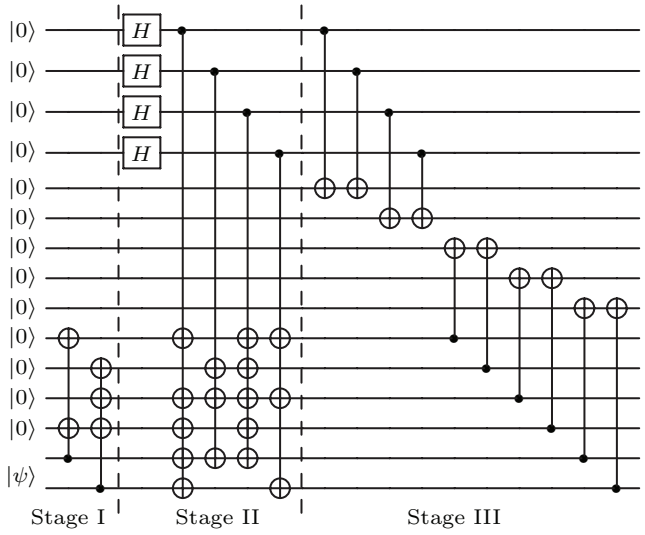


Fig. 3. The encoding circuit of the AQCC $[[15,2,6/3]]$.

4. Discussion and conclusions

In this paper, we constructed new families of AQCCs based on the concatenation scheme by utilizing error degeneracy of quantum codes. We made detailed comparisons between our new codes and previous AQCs, and showed that our codes can have a better performance than previous ones. Several families of highly degenerate AQCCs with a large asymmetry were deroved. We gave the general encoding circuit of AQCCs and showed that the number of quantum gates needed to encode our codes is lower than that of the general stabilizer codes. Our codes are practical to the future quantum information processing systems[33,34] with highly biased errors.

References

[1] Tang G Z, Sun S H and Li C Y 2020 *Chin. Phys. Lett.* **36** 070301
[2] Tian Y L, Feng T F and Zhou X Q 2019 *Acta Phys. Sin.* **68** 110302 (in Chinese)
[3] Cheng X, Zhao Y C, Y C Wu and Guo G P 2021 *Chin. Phys. Lett.* **38** 030302
[4] Ketkar A, Klappenecker A, Kumar S and Sarvepalli P K 2006 *IEEE Trans. Inf. Theory* **52** 4892
[5] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University) pp. 426–510
[6] Dumer I, Kovalev A A and Pryadko L P 2015 *Phys. Rev. Lett.* **115** 050502
[7] Sarvepalli P K, Klappenecker A and Rötteler M 2009 *Roy. Soc. A* **465** 1645
[8] Tuckett D K, Darmawan A S, Chubb C T, Bravyi S, Bartlett S D and Flammia S T 2019 *Phys. Rev. X* **9** 041031
[9] Ezerman M F, Jitman S, Kiah H M and Ling S 2013 *Int. J. Quantum Inf.* **11** 1350027
[10] Wang L, Feng K, Ling S and Xing C P 2010 *IEEE Trans. Inf. Theory* **56** 2938
[11] Galindo C, Geil O, Hernando F and Ruano D 2017 *IEEE Trans. Inf. Theory* **64** 2444
[12] Christensen R B and Geil O 2020 *Finite Fields Appl.* **68** 101742
[13] Aliferis P and Preskill J 2008 *Phys. Rev. A* **78** 052331
[14] Brooks P and Preskill J 2013 *Phys. Rev. A* **87** 032310
[15] Tuckett D K, Bartlett S D and Flammia S T 2018 *Phys. Rev. Lett.* **120** 050505
[16] Tuckett D K, Bartlett S D, Flammia S T and Brown B J 2020 *Phys. Rev. Lett.* **124** 130501
[17] Nadkarni P J and Garani S S 2017 *Proceedings of the* 2017 *IEEE Information Theory Workshop*, November 6–10, Kaohsiung, Taiwan, p. 219
[18] Nadkarni P J and Garani S S 2020 *IEEE Trans. Quantum Eng.* **1** 2101417
[19] Lin S and Costello D J 2004 *Error Control Coding: Fundamentals and Applications* (New Jersey: Prentice-Hall) p. 739
[20] Fan J H, Li J, Wang J X, Wei Z H and Hsieh M H 2021 *IEEE Trans. Commun.* **69** 3971
[21] Christandl M and Müller-Hermes A 2021 *Proceedings of the* 24*rd Annual Conference on Quantum Information Processing*, February 1–5, 2021, Munchen, Germany, p. 233, arXiv: 2009.07161
[22] Ezerman M F, Jitman S, Ling S and Pasechnik D V 2013 *IEEE Trans. Inf. Theory* **59** 6732
[23] Calderbank A R and Shor P W 1996 *Phys. Rev. A* **54** 1098
[24] MacWilliams F J and Sloane N J A 1981 *The Theory of Error-Correcting Codes* (Amsterdam: North-Holland 1981) p. 93
[25] Maucher J, Zyablov V V and Bossert M 2000 *IEEE Trans. Inf. Theory* **46** 642
[26] Guardia G G La 2012 *Quantum Inf. Process.* **11** 591
[27] Guardia G G La 2014 *Int. J. Theor. Phys.* **53** 2312
[28] Grassl M 2007 *Bounds on the minimum distance of linear codes and quantum codes*, Online available at http://www.codetables.de, 2007
[29] Ezerman M F, Ling S and Sole P 2011 *IEEE Trans. Inf. Theory* **57** 5536
[30] Ashikhmin A, Litsyn S and Tsfasman M A 2001 *Phys. Rev. A* **63** 032311
[31] Gottesman D 1996 *Phys. Rev. A* **54** 1862
[32] Grassl M, Beth T and Rötteler M 2004 *Int. J. Quantum Inf.* **2** 55
[33] Zhu X Y, Tu T, Guo A L, Zhou Z Q and Guo G C 2020 *Chin. Phys. Lett.* **37** 020302
[34] Gong B, Tu T, Guo A L, Zhu L T and Li C F 2021 *Chin. Phys. Lett.* **38** 044201